הדור הראשון של הכופרות: מבוא לדור השני

מאת עו"ד יהונתן קלינגר

כופרות הן השם החזק בתחום אבטחת המידע בשנה האחרונה.

עד היום לא תמיד היה מודל עסקי לוירוסים. החל משנות ה-80 המוקדמות אנשים תהו למה לפתח וירוסים ולמעט מספר מצומצם של וירוסים ששימשו ארגוני מודיעין להשבתת תשתיות קריטיות של מדינות אויב על פי מקורות זרים, הרי שאין באמת הצדקה כלכלית לפיתוח של וירוסים. בעבר, אדם היה כותב וירוס שגורם לנזק כלשהו (לדוגמא וירוס פינג-פונג ששיחק פינג פונג על המסך של אדם מסוים), אבל לא היה יכול להתפרנס מהוירוס שכתב. מי שהתפרנסו ויפה מאותם וירוסים היו חברות האנטי-וירוס שהיו יכולות למכור תוכנות יעילות יותר ויותר כל מספר חודשים כדי לעצור את הוירוסים. הכניסה של וירוסים המאפשרים מוניטיזציה, הכנסות כלכליות ממשיות, בזכות ההדבקה, לא היתה מתאפשרת אלא באמצעות מספר התפתחויות טכנולוגיות שקמו בשנים האחרונות.

ההיסטוריה של הוירוסים, באמת בקצרה: וירוסי מחשב החלו להופיע כתופעה בשנות השמונים, כאשר מדובר היה ברכיבי קוד המשכפלים את עצמם ומפיצים עצמם ברשת או באמצעות התקני אחסון וגורמים לנזק או לשיבוש חומר המחשב. מספר דוגמאות לוירוסים ידועים לשמצה הן וירוס מיכאלאנג'לו אשר השבית את המחשב ביום הולדתו של האמן המפורסם, וירוס פינג-פונג, שהפך את מסך המחשב ללוח משחקים ווירוס יום שישי ה-13 אשר השבית מחשבים ומחק קבצים בתאריך זה. הוירוסים באותה תקופה היו פשוטים יחסית ובהעדר קישוריות לאינטרנט הדרך שבה הדביקו מחשבים אחרים היתה על ידי העברת דיסקטים, כלומר, אזור ה-BOOT בדיסקט הודבק על ידי הוירוס, שהיה "מדביק" את מערכת ההפעלה ולאחר מכן גם כל דיסקט נוסף. ההתפשטות בצורה כזו היא אמנם איטית ופרימיטיבית ביחס לוירוסים של היום, אולם בהתחשב בכך שבאותה תקופה לא היו רשתות תקשורת נפוצות ולא היו עדכונים רבים למערכות הפעלה והדרך שבה אנשים העבירו קבצים אחד לשני היו באמצעות דיסקטים. – הוירוסים עדיין זכו לתפוצה רחבה מאוד.

ההתפשטות באמצעות דיסקטים ומערכות CD ROM בשנות השמונים והתשעים של המאה הקודמת היו דרך קלה להדבקת מחשבים ויצרו תעשיה של תוכנות אנטי-וירוס, שגם הן, בדרך כלל, הופצו בצורה לא חוקית על ידי דיסקטים. הגאווה הציונית של כרמל אנטי-וירוס היתה מופצת על דיסקטים בין אדם למשנהו ומועתקת גם היא. מה היתה הבטוחה שיחד עם תוכנת האנטי וירוס לא יתקבלו וירוסים נוספים? ככל הנראה אין. תוכנות האנטי-וירוס של פעם היו פשוטות: הן חיפשו וירוסים מתוך רשימה ידועה והן עבדו על איזורים ספציפיים בדיסק הקשיח או הזכרון לאתר אותם. תוכנות האנטי-וירוס הישנות היו יעילות בזמנו וכנראה שלא היו יעילות היום.

השינויים בשנות ה-2000 המוקדמות: עם בוא שנות ה-2000 התחברו יותר ויותר אנשים לרשת והוירוסים הפכו לכאלה שדורשים התגברות על שני חסמים: הראשון הוא עדכוני תוכנה ואבטחה (עד לחיבור לרשת, אנשים כמעט ולא עדכנו את מערכות ההפעלה שלהם) והשני הוא הפצה באמצעים שאינם דיסקטים. לכן, החלו לצוץ וירוסים הפועלים על הרשת. אחד שזכור הוא וירוס בלאסטר משנת 2003. אותו וירוס (או תולעת, תלוי את מי שואלים), ניצל פרצת אבטחה ב-RPC של מערכת ההפעלה חלונות XP וגרם לכך שכל מחשב שנדבק בוירוס יצר פניות ברשת והתקפות על מחשבים נוספים כך שהוא הדביק גם אותם. כל מחשב שהיה מחובר לאינטרנט ולא סגר את פרצת האבטחה במערכת ההפעלה הודבק וכך בעצם הוירוס התפשט בקלות ברשתות. זה כמובן לא היה הוירוס היחיד והיתרון שלו היה שהוא לא דרש העתקה פיסית של כוננים אלא ביצע את ההתפשטות בצורה כזו.

רושעות: בהתבסס על כלים רבים שנלמדו בתעשיית הוירוסים, החלו להתפתח תוכנות רבות שמוגדרות "רושעות" (malware) תוכנות אלו היו זדוניות אך לא במובן נטול האינטרסים של מחוללי הוירוסים התמימים עד כה. אותם סרגלי כלים, תוכנות ששינו את עמודי הבית בדפדפן והתקינו תוכנות פעלו ממטרות כלכליות נטו. תוכנות סרגלי הכלים וכל הנלוות להם עבדו בצורה כמעט זהה לוירוסים: הן הדביקו משתמשים בתוכנות לא רצויות. חלק מהן היו מקפיצות חלונות פרסומות, חלק היו מחליפות את מנוע החיפוש בדפדפן וחלקן היו פשוט לוקחות את החופש להתקין לך עוד תוכנות על המחשב. עולם הרושעות יצר כלכלה משמעותית בישראל וקיבל את הכינוי "Download Valley" ובשיאו היה שווה מיליארדי דולרים. הרושעות הללו פותחו על ידי חברות לגיטימיות לגמרי (חלקן נסחרו בבורסה) והתפרנסו על ידי תיווך בין אנשים שרצו לקדם את התוכנה שלהם ובין משתמשי קצה שיודעים ללחוץ על כפתור ה-"Next" בלבד.

בועת הרושעות שהחלה בשנות ה-2000 המאוחרות התבססה על אנשי אבטחת מידע שידעו להשתמש בפרצות האבטחה אותן הכירו במהלך העבודה כדי לעקוף הגנות של חוסמי פרסומות, אנטי וירוסים ותוכנות הגנה שונות. כל אלו הביאו לא רק מוניטין רע לתעשיית הפרסום, אלא גם רעיונות עסקיים לפתרונות יצירתיים יותר או פחות. לדוגמא, תוכנת התקנה מסוימת ידעה לזהות מתי היא רצה במכונה וירטואלית ולהמנע מלהציג פרסומות בתהליך ההתקנה, מתוך הבנה שצוותי מחקר יפעילו אותה על מכונות וירטואליות. באותה התקנה דובר גם על שימוש בתעודות (certificate) כדי לייצר נופך של אמינות.

רושעות רחוקות מלהיות וירוסים. מדובר על תוכנות לא רצויות שמשתמשות בטריקים והרבה פעמים בטקטיקות שהן על גבול החוקי כדי לקדם הכנסות, אך הן עדיין לא מבצעות משהו פלילי. אולם, הן היו צעד חשוב בהגעה המתבקשת והמתחייבת לכופרות. הצעד הבא אחריהן היה, כמובן, הביטקוין.

ביטקוין: בשנת 2009 נכנס הביטקוין להיסטוריה בתור המטבע המבוזר הקריפטוגרפי הראשון. ביטקוין הוא מטבע שמאפשר תשלום בין כל אדם לחברו באמצעות מערכת מבוזרת המאוחסנת על מחשבים של צמתים ברשת. מדובר על כסף בקוד פתוח, מערכת שמאפשרת תשלומים ללא בנק מרכזי, ללא חשבון שניתן לעקל וללא גורמי ביניים שיכולים לתפוס את הכסף. מאז 2009 התפתח המטבע ובשנת 2011 הבורסה MTGOX איפשרה מסחר ורכישה של המטבע בדולרים וההפך. היתרון בביטקוין הוא שבעוד

שהעסקאות עצמן מופיעות בכל מחשב וזמינות לכל אחד, הרי שלדעת את זהות המשתמש בכסף קשה מאוד. כך, אם ישולם לי סך של 100$ בביטקוין, איש לא יוכל לדעת מי אני וכל עוד אני לא אתחקה אחר כל העסקאות ברשת ביטקוין, (דבר שקשה יחסית) לא אוכל לדעת מי האדם שקיבל ממני את הכסף גם אם יגיע לאחד משירותי החלפנות.

האפשרות לקבל כסף אנונימי ולא דרך הבנק, ביחד עם היכולת להתקין לאנשים תוכנה על המחשב ובסופו של דבר יחד עם כל ההתפתחויות הטכולוגיות האחרות שתוארו, היו מה שהביאו לכר המצע החם שאיפשר להקים את עולם הכופרות.

כופרות, מהן: כופרה (ransomware) היא שקלול שלא היה יכול לבוא לעולם אלא אם כל התנאים הנכונים התקיימו. התנאי הראשון הוא כלים שיאפשרו התפשטות ברשת באמצעות פרצות אבטחה קיימות, התנאי השני הוא אפשרות לשלם בצורה אנונימית והשלישי הוא קיומה של תשתית מאובטחת מספיק כדי לוודא את התשלום ולאפשר שחרור אוטומטי של הקבצים בעת התשלום (להבדיל משחרור ידני). אז איך תוכנת כופר עובדת? התוכנה משתלטת על המחשב כמו כל וירוס או תוכנה זדונית ומצפינה את כל הקבצים באמצעות מפתח פרטי שידוע למפתח התוכנה.

בשלב הבא, מופיעה הודעה לבעל המחשב כי כל הקבצים שלו הוצפנו ודורשת תשלום; מופיעה כתובת של ארנק ביטקוין לתשלום אשר התשלום אליה ישחרר את הקבצים.

רגע של היסטוריה: עוד בשנת 2006, לפני הבשלת הטכנולוגיות הרלוונטיות, היתה תוכנת כופר בשם Cryzip. התשלום עבור שחרור הכופר היה באמצעות שירות e-gold, שירות שאינו אנונימי לגמרי אך סיפק הגנה טובה יחסית למפתח התוכנה. בפועל, השירות לא היה אנונימי וכל העסקאות תועדו; מעבר לכך, לא היתה אפשרות (מעשית) להוציא את הכספים החוצה בלי להחשף לרשויות הבטחון.

בשלב הזה רוב הקוראים יגידו "היי, אבל הקבצים שלי שמורים גם בענן" ובכן, חלק מתוכנות הכופר טיפה יותר חכמות מזה ואף מצפינות את הקבצים בשירות הענן ומוחקות גיבויים או סתם משחיתות את הקובץ, כך שאין אפשרות לשחזר מהגיבוי.

אז נחזור לבעיה: הבעיה של תוכנות הכופר היא שהן משתלטות על מערכות מחשב בצורה קלה מדי. לפי חברת האבטחה McAfee, התקנות של כופרה מבוצעות בדיוק באותן הדרכים שבהן מותקנים סרגלי כלים ושאר רושעות: על ידי דואר אלקטרוני שמכיל לינקים זדוניים, על ידי תשלום לסרגלי כלים לעודד את ההתקנה ועל ידי פרצות אבטחה בדפדפנים שמבצעים התקנת תוכנה ברקע. מרגע שהתוכנה השתלטה על המחשב, היא יכולה לשבת רדומה על המחשב כדי להמתין לרגע הנכון, למחוק גיבויים ולנטרל את הסדרי האבטחה.

כופרות אינן רק מיועדות למחשבים אישיים; יש כופרות שמבצעות את אותו ה"שירות" על שרתי אינטרנט ומעלימות אתרי אינטרנט שלמים מהאוויר עד לתשלום הכופר. בישראל לא מעט גורמים בשוק חוו השתלטות של כופרה והדבר יצר נטל משמעותי על המשק בשנה האחרונה, מחשב במשרד ראש הממשלה, עיריית נצרת עילית, משרדי עורכי דין ומאות ארגונים אחרים שצריכים לנהל מערך מאובטח, נדבקו בתוכנות כופר ושילמו, הכל כדי להציל את המידע היקר שלהם.

המלצות רשויות הבטחון: בתחילה, ה-FBI המליץ לאזרחים לשלם לתוכנות כופר כדי לשחרר את הקבצים שלהם. ההמלצה של משטרת ישראל (ושל ה-FBI כיום) היתה לא לשלם לתוכנות כופר שכן הדבר מקדם את פיתוח הדור הבא של תוכנות הכופר ומאפשר התעשרות של עבריינים. הסיבה היחידה שעבריינים ממשיכים לפתח תוכנות כופר היא כיוון שהדבר רווחי; ככל הנראה, כל עוד אחוז המשלמים גבוה מספיק, זה ישתלם להמשיך להפיץ ולפתח כופרות. אם אף אחד לא ישלם על כופר, אז לא יהיה תמריץ להמשיך לנסות להדביק והתופעה תגמר (בדיוק כמו בעולם החיסונים, הכמות האופטימאלית של חיסון היא 1100%).

כאן נוצר מצב שהתמריץ הקולקטיבי הוא לא לשלם לתוכנות כופר, כיוון שהתשלום לתוכנות כופר פוגע בחברה ככלל, אבל ליחיד עצמו יש תמריץ לשלם כיוון שהנזק שנגרם לו כרגע הוא יותר גבוה אם הוא לא ישלם מאשר אם הוא ישלם. הדילמה הזו, שנקראת "דילמת האסיר" מסבירה טוב מאוד מדוע כולם, בסופו של דבר, משלמים: הנזק שנגרם לפרט אם הוא לא משלם הוא, לצורך העניין, 5,000 דולר (שעות עבודה הנדרשות על מנת לשחזר את המסמכים היקרים בארגון), המחיר של הכופר הוא, נניח, 1,000 דולר. התועלת לכלל החברה אם הוא לא משלם היא מיליארדי דולרים והמחיר של לא לשלם הוא נמוך יותר מזה. הבעיה היא שאף אחד לא רואה את התמונה הכללית ולכן כל אחד מהארגונים שנדבק בתוכנות כופר אמור להיות אנוכי ולשלם עבור שחרור הקבצים שלו.

דבר שאם לא תהיתם עד עכשיו כדאי שתתהו, הוא למה לעזאזל לשלם? מאיפה אנחנו יודעים שאותם גופים בכלל ישחררו את הקבצים אם נשלם, הרי הם פושעים: אכן, כמה מתוכנות הכופר בכלל מחקו את הקבצים לאחר ששילמת את הכופר, חיפוש של שם הכופרה ברשת בדרך כלל מניב תוצאות שמעידות על האם הקבצים ישוחררו או לאו; בחלק מהמקרים יש מפתחי תוכנה שמתהדרים במוניטין שלהם ולא יסכנו אותו (ואת אחוזי ההמרה) על ידי אי שחרור. היו כמה מקרים בהם שולם הכופר אך לא השתחררו קבצים והדבר מעיד ומחזק את ההמלצה שלא לשלם לתוכנות כופר כלל וכלל.

העניין הוא שבתיאוריה לגמרי ניתן לייצר מערכת מאובטחת שתוודא כי מי שמשלם אכן מקבל את הקבצים שלו בחזרה וזה קצת הזוי: ניתן לעשות זאת בצורה שתהיה מאוד תמוהה, אבל היא דורשת שחרור של קוד המקור של תוכנת הכופר בפלטפורמה מוכרת כמו GitHub וכן שימוש בטכנולוגיית MultiSig בביטקוין כדי לוודא כי התשלום ישוחרר רק לאחר פתיחת הקבצים. הקוד יעבוד כך: בשלב הראשון הוא יחולל מפתח פרטי של העבריין ומפתח פרטי של הלקוח, הוא יצפין את כל הקבצים עם המפתח הפרטי של העבריין וינעל את הקבצים הרלוונטיים. הוא יצור כתובת תשלום המאפשרת שחרור

הקבצים רק באמצעות המפתח הפרטי של שני הצדדים. בשלב השני, התוכנה תוודא כי אכן בוצע התשלום לכתובת המשותפת (Multisig) ותדאג לשחרר את הקבצים כאשר היא תזהה את התשלום המבוצע לתוך הארנק המשותף

בשלב האחרון, לאחר שזיהתה התוכנה כי כל הקבצים שוחררו והמערכת שבה למצב תקין, היא תעביר את התשלום מהארנק המשותף לארנק של העבריין.

מערכת כזו, הגם שהיא פלילית לגמרי והיא וירוס לכל דבר, מאפשרת יצירת אמון במערכות כופר כך שתמנע ניצול לרעה והותרת קרבנות שחוו הן אבדן של קבצים יקרים והן אבדן של כסף. אכן, ניתן יהיה לנצל את המערכת לרעה ולהגדיל את כלכלת הוירוסים, אך בפועל ניתן יהיה גם להקטין את הנזק שנגרם לחברה כתוצאה מאי שחרור הקבצים על ידי תוכנות שנכתבו מראש כך שלא פעלו לשחרור הקבצים.

היתרון בשימוש בקוד פתוח במקרה כזה הם שמרגע שהקוד ידוע, מרגע שניתן לוודא כי הקוד שנעל את הקבצים הוא אכן הקוד שמופיע באתר, ניתן אף לאמת את החתימה של הוירוס ולוודא כי אכן תקבל את הכסף בחזרה. ה"יתרון" הנוסף לכך, הוא שבניגוד לכופרות רגילות, שהן קנייניות ועל מנת לפתח תוכנות שנועדו להגן מהן או לפתוח את ההצפנה שלהן נדרש לפרוץ למערכות המחשב, כאן התחרות היא בקלפים פתוחים, בקוד פתוח, בעולם שבו ניתן לשחק בצורה הוגנת: כל אחד יודע מי העבריינים וכיצד אפשר לבטוח בהם שיהיו הוגנים למרות שהם עוברים על החוק.

הבעיה העיקרית בתוכנות כופר היא שהיא מצאה מודל עסקי חדש לעולם אבטחת המידע: היא מצאה דרך לגבות "קנס" מארגונים שאינם מאבטחים את המידע שלהם כראוי ורק חבל שהקנס הזה מועבר לארגוני פשיעה ולא לגורמים שנועדו לאכוף את החוק ולהגן על המידע האישי שלנו. אם המצב ההזוי והמוזר היה כזה שבו רשות ממשלתית שמקדמת אבטחת מידע היתה מפיצה וירוס כזה כדי להטיל קנסות על גופים שלא יאבטחו את המידע שלהם כראוי, הרי שהיתה מדוברת בבדיקת האבטחה הטובה בהיסטוריה.

ואגב בדיקת האבטחה הטובה בהיסטוריה, לאחרונה נרשמה חברה בריטית בשם drop table ; companies